#4

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されてる事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed h this Office.

出 願 年 月 日
ate of Application: １９９９年 ９月２４日

願 番 号
plication Number: 平成１１年特許願第２７１０２２号

願 人
licant (s): 溝部 達司
澤口 高司

２０００年 ８月 ４日

特許庁長官
Commissioner,
Patent Office 及川耕造

【書類名】　特許願

【整理番号】　SM199909

【提出日】　平成11年 9月24日

【あて先】　特許庁長官　殿

【国際特許分類】　G06K 9/00

G06F 15/62

【発明者】

【住所又は居所】　東京都新宿区高田馬場３－４０－１３

【氏名】　澤口　高司

【特許出願人】

【識別番号】　000168207

【氏名又は名称】　溝部　達司

【特許出願人】

【識別番号】　596132905

【氏名又は名称】　澤口　高司

【代理人】

【識別番号】　100064414

【弁理士】

【氏名又は名称】　磯野　道造

【手数料の表示】

【予納台帳番号】　015392

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9722612

【包括委任状番号】　9607741

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　携帯個人認証装置及び同装置によりアクセスが許可される電子システム

【特許請求の範囲】

【請求項１】　携帯可能に構成され、通信手段を内蔵すると共に、人間の生物学的特徴のうち少なくとも一つを読み取る読取手段を有し、この読み取ったデータを認証データとして、この認証データに基づいて個人の認証を行うこと、を特徴とする携帯個人認証装置。

【請求項２】　前記認証が、人間の指紋、声紋、網膜紋、虹彩紋、顔、署名、のうち少なくとも一つを利用したバイオメタリクス認証であり、

前記読取手段はこのバイオメタリクス認証に対応して、人間の指紋、声紋、網膜紋、虹彩紋、顔、署名、のうち少なくとも一つを読み取ることができるものであること、

を特徴とする請求項１に記載の携帯個人認証装置。

【請求項３】　前記携帯個人認証装置は、個人認証を前提として利用者のアクセスが可能となる電子システムにおける個人認証に使用され、

前記読み取った認証データにより、前記電子システムの利用を意図する利用者がこの電子システムへのアクセスの許可を受けること、

を特徴とする請求項１又は請求項２に記載の携帯個人認証装置。

【請求項４】　前記電子システムが通信ネットワーク上を流通する電子情報に貨幣的価値を与えて電子貨幣を設定し、この電子貨幣により商取引の決済を行う電子商取引システムであり、

前記携帯個人認証装置は、この電子商取引システムが要求する個人認証のための認証データの入力を行うと共に、

所定の金融機関の口座から所定の金額の預貯金を引き出し、これを電子貨幣として記憶部に格納し、この格納した電子貨幣により前記商取引の決済を行うこと、ならびに前記決済後の電子貨幣の残高及びその使用履歴を前記格納部に残すこと、

を特徴とする請求項１乃至請求項３のいずれか１項に記載の携帯個人認証装置。

【請求項５】　前記電子システムがクレジット情報により決済を行う電子商取引システムであり、

前記携帯個人認証装置は、この電子商取引システムが要求する個人認証のための認証データの入力を行うと共に、

クレジット情報が格納される格納手段を有すること、

を特徴とする請求項１乃至請求項３のいずれか１項に記載の携帯個人認証装置。

【請求項６】　前記電子商取引システムが通行料金を自動的に徴収する自動料金収受システムであることを特徴とする請求項４又は請求項５に記載の携帯個人認証装置。

【請求項７】　前記電子システムが緊急事態発生時に所轄のセンタに緊急連絡を行う通報システムであり、

前記携帯個人認証装置は、少なくとも前記緊急連絡を解除する際の解除連絡に使用され、

前記解除連絡を行う際には、この携帯個人認証装置により読み取った認証データを前記通信手段により前記所轄のセンタに送信すること、

を特徴とする請求項３に記載の携帯個人認証装置。

【請求項８】　前記生物学的特徴の一つを指紋とし、前記携帯個人認証装置はＰＣカードスロットを有し、このＰＣカードスロットに前記指紋を読み取る読取手段を備えたＰＣカードを挿入することで本人の認証を行うことを特徴とする請求項１乃至請求項７のいずれか１項に記載の携帯個人認証装置。

【請求項９】　請求項３乃至請求項８のいずれか１項に記載の携帯個人認証装置によりアクセスが許可される電子システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、もっぱら個人の認証を行ったり個人認証を前提とする電子システムなどに使用される携帯個人認証装置及び同装置によりアクセスが許可される電子システムに関し、例えば、セキュリテイ管理、電子商取引、あるいは、自動車事故、海山における遭難事故等における緊急連絡に用いて好適な、携帯個人認証装

置及び同装置によりアクセスが許可される電子システムに関する。

【０００２】

【従来の技術】

従来から現金の代用として、所定の電子データを個人情報とともにＩＣカード、クレジットカード、デビットカード、スーパーカード等に記憶させ、その電子データの交換によって支払いを行う電子決済システムが知られている。

一方、最近では、インタネット等通信ネットワークを用いた電子商取引が実現しつつある。これに伴い、電子商取引に関する決済をネットワーク上で行う技術が各種提案されている。代表的には、クレジットカード決済であり、あるいは、実際の紙幣と同じ価値を持つ電子マネーを用いたキャッシュ決済である。

【０００３】

このような状況の中、誰もがインタネットに接続されているコンピュータにアクセスする可能性が生まれ、正当な利用者か、正当な情報かを判断する電子認証の重要性が高まってきている。加えて企業がインタネットを商取引等重要な業務に利用し始めたため、ネットワーク社会での電子的な身分証明は必須となっている。

【０００４】

また、最近、自動車のエアバックの作動を契機として、その事故情報を消防署や警察、保険会社等所轄のセンタに緊急連絡する通報システムが実現されようとしている。ところが、エアバックが作動しても事故が軽微なこともあり、機器の誤動作もある。事故が軽微な場合、本人がその緊急連絡システムを解除すれば問題ないが、大事故の場合に、誰かが故意に、あるいは誤って解除することが有り得る。この場合、連絡した人間が本人であるか否か等の認証が重要になる。

【０００５】

【発明が解決しようとする課題】

上述した電子商取引において、ＩＣカード等の記憶媒体を用いて電子決済を行う場合、あるいはクレジットカードによる決済を行う場合は、第三者による不正使用を防御するため、利用の都度パスワード入力による利用者の認証が必要となり、操作や処理が煩雑となる欠点があり、また、防御をかけない場合は、そのＩ

Ｃカード等に設定された金額の全てが第三者による不正使用の危険にさらされるといった欠点を有している。

【０００６】

また、インタネットを用いて電子商取引を行う場合、前者は、クレジットカードを必要とし、カード番号等セキュリテイを必要とする情報をなんらかの方法により送信する必要があり、ＩＣカードを利用して電子決済を行うのと同じ欠点を持つ。

更に、上述した自動車事故等の通報システムにおいても同様、緊急連絡解除の際に信用性の高い本人認証のための手段が要求され、通報あるいは通報解除の確度が高いものが期待される。

上記に限らず、どこでも簡便に個人の認証を行うことのできる手段が、今後必要になると考える。また、カード社会においてはカードが氾濫し、何枚ものカードを携帯しなければをらない煩わしさや、カードを管理しなければならない煩わしさがある。

そこで、本発明は、上記課題を解決し、今後の社会において必要不可欠となる個人の認証をどこでも行え、あらゆる用途に使用することのできる携帯個人認証装置及び同装置によりアクセスが許可される電子システムを提供することを目的とする。

【０００７】

【課題を解決するための手段】

上述した課題を解決した請求項１に記載の携帯個人認証装置は、携帯可能に構成され、通信手段を内蔵すると共に、人間の生物学的特徴のうち少なくとも一つを読み取る読取手段を有し、この読み取ったデータを認証データとして、この認証データに基づいて個人の認証を行うことを特徴とする。

この携帯個人認証装置は、今後一人一台程度所持するであろう携帯電話やＰＤＡなどの携帯機器をベースとして構成したり、携帯電話やＰＤＡの機能を併せ持たせるのが好適である。個人の認証を行うに際しては、入力された認証データ（読み取ったデータ）とあらかじめ登録してある参照データとを対比することになるが、あらかじめ登録してある参照データは、携帯個人認証装置内に格納される

こととしても良い。また、あらかじめ登録してある認証データは、携帯個人認証装置以外の例えばサーバ（発明の実施の形態でいう「認証サーバ」）などに格納されることとしても良い。この場合は、例えば、入力された認証データを通信手段によりサーバ側に送信し、サーバ側で行った認証結果を通信手段により得る。この携帯個人認証装置は、例えば、警察における不審者尋問や警備会社などにおける警備に用いることができる。また、これに限らず広く個人の認証に用いることができる。

なお、通信手段は、有線・無線を問わない。

【０００８】

また、請求項２に記載の携帯個人認証装置は、前記認証が、人間の指紋、声紋、網膜紋、虹彩紋、顔、署名、のうち少なくとも一つを利用したバイオメタリクス認証であり、前記読取手段はこのバイオメタリクス認証に対応して、人間の指紋、声紋、網膜紋、虹彩紋、顔、署名、のうち少なくとも一つを読み取ることができるものであることを特徴とする。

これらは、個人に特有のものであり、パスワードのごとく個人が記憶しておく必要がない。また、カギなどの物品のごとく置き忘れるということもない。読取手段としては、声紋に対してはマイクロフォンが、指紋、網膜紋、虹彩紋、顔、署名に対してはＣＣＤカメラが、指紋、署名に対してはスキャナがあげられる。

【０００９】

また、請求項３に記載の携帯個人認証装置は、個人認証を前提として利用者のアクセスが可能となる電子システムにおける個人認証に使用され、前記読み取った認証データにより、前記電子システムの利用を意図する利用者がこの電子システムへのアクセスの許可を受けることを特徴とする。

前記のとおり個人の認証を行うに際しては、入力された認証データ（読み取ったデータ）とあらかじめ登録してある参照データとを対比することになるが、あらかじめ登録してある参照データは、携帯個人認証装置内に格納されることとしても良い。この場合は、認証結果を電子システムに送信する。あるいは、認証結果を携帯認証装置に表示する。また、あらかじめ登録してある認証データは、電子システムが有するサーバなどに格納されることとしても良い。この場合は、例

えば、入力された認証データを電子システム側に送信する。

なお、特許請求の範囲における用語「アクセス」には、発明の実施の形態のように、ＳＯＳ信号を解除するために通信を行い、該ＳＯＳ信号を解除する行為なども含まれる。また、特許請求の範囲における用語「電子システム」は、電子商取引システム、道路や駐車場などの自動料金収受装置、自動販売機、公衆電話回線（ＩＳＤＮを含む）、パソコン、ＬＡＮ（有線・無線）、インタネットなどがあげられる。ちなみに、自動販売機の場合には、例えば有線（又は無線）で携帯個人認証装置と自動販売機を接続し、携帯個人認証装置側で認証データを入力し（読み取り）、この入力された認証データを自動販売機に送信して、取引可能とする構成とすることができる。また、ＬＡＮの場合は、端末のパソコンに携帯個人認証装置を有線（又は無線）で接続し、携帯個人端末装置側で認証データを入力し、この入力された認証データをパソコン側に送信し、パソコンあるいはサーバで判断して、パソコンの使用及び／又はサーバへのアクセスを可能とする構成とすることができる。

【００１０】

また、請求項４に記載の携帯個人認証装置においては、前記電子システムが通信ネットワーク上を流通する電子情報に貨幣的価値を与えて電子貨幣を設定し、この電子貨幣により商取引の決済を行う電子商取引システムであり、前記携帯個人認証装置は、この電子商取引システムが要求する個人認証のための認証データの入力を行うと共に、所定の金融機関の口座から所定の金額の預貯金を引き出し、これを電子貨幣として記憶部に格納し、この格納した電子貨幣により前記商取引の決済を行うこと、ならびに前記決済後の電子貨幣の残高及びその使用履歴を前記格納部に残すこと、を特徴とする。

なお、この携帯個人認証装置を携帯通信端末装置として持つ電子商取引システムは、通信ネットワーク上を流通する電子情報に貨幣的価値を与えて電子貨幣を設定し、この電子貨幣により商取引の決済を行う電子システムであり、個人の認証を前提としている。

この電子貨幣の種類としては、ＩＣカード型、ネットワーク型のどちらも含むものであり、特に限定しない。また、この電子貨幣の種類としては、クローズド

型、オープン型のどちらも含むものであり、特に限定しない。なお、オープン型の電子貨幣は、使用された後、すぐに決済されて現金化されずに、他人に移転することができる電子貨幣である。

【００１１】

また、請求項５に記載の携帯個人認証装置においては、前記電子システムがクレジット情報により決済を行う電子商取引システムであり、前記携帯個人認証装置は、この電子商取引システムが要求する個人認証のための認証データの入力を行うと共に、クレジット情報が格納される格納手段を有することを特徴とする。

なお、この携帯個人認証装置を携帯通信端末装置として持つ電子商取引システムは、前記商取引の決済をクレジット方式で行う電子システムであり、個人の認証を前提としている。

【００１２】

また、請求項６に記載の携帯個人認証装置においては、前記電子商取引システムが通行料金を自動的に徴収する自動料金収受システムであることを特徴とする。

通行料金を自動収受する自動料金収受システムとしては、ＥＴＣ（Electric Toll Collection）が知られる。携帯個人認証装置により、自動車に搭載されるＥＴＣの車載装置の作動を可能とする（自動料金収受の認証を行う）。

あるいは、ＥＴＣの路上装置と携帯個人認証装置とで直接通信を行う構成とすることもできる。この場合、ＥＴＣの車載装置が不用になる。

【００１３】

また、請求項７に記載の携帯個人認証装置においては、前記電子システムが緊急事態発生時に所轄のセンタに緊急連絡を行う通報システムであり、前記携帯個人認証装置は、少なくとも前記緊急連絡を解除する際の解除連絡に使用され、前記解除連絡を行う際には、この携帯個人認証装置により読み取った認証データを前記通信手段により前記所轄のセンタに送信することを特徴とする。

なお、この携帯個人認証装置を携帯通信端末装置として持つ電子システムたる通報システムは、例えば、車両などに全地球測位システムの衛星電波を受信する機器を搭載し、緊急事態発生時に管轄センタに緊急連絡を行う。この通報システ

ムは、緊急事態発生時、前記搭載機器により、少なくとも前記衛星電波により測位された現在位置データを携帯通信回線ネットワーク経由で発信して緊急連絡を通報する。この通報システムにおける緊急連絡の通報の解除は、携帯個人認証装置により前記所轄のセンタに連絡をとる。この際、携帯個人認証装置で読み取った認証データを、通信手段によりセンタに送信し、センタのサーバなどにあらかじめ登録済みの参照データと照合し、その照合結果に基づき、前記緊急連絡の解除を有効とする。

さらに、海や陸での事故並びに遭難の際に、携帯個人認証装置により、認証データを送信すると共に、緊急連絡を行う構成としても良い。緊急連絡の解除の際と同様、個人の特定・悪戯などの防止に有効である。

【００１４】

また、請求項８に記載の携帯個人認証装置は、前記生物学的特徴の一つを指紋とし、前記携帯個人認証装置はＰＣカードスロットを有し、このＰＣカードスロットに前記指紋を読み取る読取手段を備えたＰＣカードを挿入することで本人の認証を行うことを特徴とする。

【００１５】

そして、請求項９に記載の発明は、携帯個人認証装置によりアクセスが許可される電子システムである。

【００１６】

上述したように、本発明は、広く個人の認証を行うものである。また、通信ネットワーク上を流通する電子情報に貨幣的価値を与えて電子貨幣を設定し、この電子貨幣により商取引の決済を行う電子商取引の本人認証を行うための手段として、また、契約、決済のための手段として携帯通信端末装置を使用する。この携帯通信端末装置は、内蔵する通信手段を介して所定の金融機関の口座から任意の金額の預貯金を引き出し、また、これを電子貨幣として格納する格納手段を有し、この格納した電子貨幣により前記商取引の決済を行ない、決済後の電子貨幣の残高及びその使用履歴を記録する。

【００１７】

このように、携帯通信端末装置（携帯個人認証装置が兼ねる）に、従来ＩＣカ

ード等が持っていた電子財布的な機能を内包させることにより操作上の煩わしさから解放すると共に、生物学的特徴である、指紋、声紋、虹彩紋、網膜紋、顔、署名のバイオメタリクスのうち少なくとも１つを本人認証のための手段として使用することにより、セキュリテイ機能の充実がはかれる。

また、ＡＴＭ機器（一例としてのＡＴＭ機器）と接続することによって電子財布としての一元管理を実現する。更に、そのモバイル機器を使用して、銀行、証券会社、保険会社、信販会社、百貨店、スーパー、運輸等々、流通系の各企業が構築するサービスシステムを、例えば、インタネットやＡＴＭオンラインを利用して取り込み、交信することによって、発受注に関する契約、あるいは決済、契約解除等の指示を容易に行うことができる。

【００１８】

更に、交通事故、遭難事故等発生の際、所轄センタへの緊急連絡解除時の本人認証のための手段としても本発明の携帯通信端末装置を用いることができる。この場合、全地球測位システム（ＧＰＳ）の衛星電波を受信できる機器を介して現在位置等を知らせるＳＯＳ信号を携帯通信回線経由で所轄のセンタに通報するが、緊急連絡解除の際に本人認証を行い、機器の誤作動による、あるいは悪意の緊急連絡解除を防止することができ、このことにより、通報の確度が向上する。

【００１９】

【発明の実施の形態】

以下、発明の実施の形態を、図面を参照して詳細に説明する。

図１は、本発明の携帯個人認証装置が携帯通信端末装置として使用される電子商取引の一実施形態を示すブロック図である。図において、１は銀行営業店システムであり、窓口にＡＴＭ機器１１を有する。２は、証券会社、保険会社、信販会社、百貨店、スーパー、運輸等の流通系システムであり、この中に銀行が含まれることもある。流通系システム２は、流通系ホスト２１を核とし、遠隔地にＰＯＳ端末２１が分散配置されている。

【００２０】

３は銀行計算機センタであり、銀行ホスト３１を核に各銀行営業店システム１とは専用回線４を介して接続されている。また、エンドユーザは、本人認証のた

めにあらかじめ指紋が採取され、その情報は認証サーバ３２に格納されてあるものとする。利用の都度、この認証サーバ３２による本人照合が行われ、セキュリテイの保護がなされる。

【００２１】

以下に示す実施形態では本人照合のための手段として、犯罪捜査等において実績のある指紋を使用するものとするが、他に個人の識別を確実に行えるものとして声紋、虹彩紋、網膜紋があり、そのいずれを用いても構わない。参考のために、指紋、声紋、虹彩紋について定義すると、指紋とは、指頭の掌側面に見られる皮膚隆線のなす紋理をいい、その形状から弓状紋、蹄状紋、渦状紋に大別される。各紋型の出現頻度には、指種、左右、性別、人種等により差異がある。指紋は、胎生３～４カ月で形成され、その形態は、全く同じものは２つとなく、また、一生不変であることから個人の識別に利用される。

声紋とは、人間の声を周波数分析した結果をソナグラフで表したものをいう。また、虹彩紋とは、眼球の水晶体の前面にあって瞳孔を囲む輪状の膜である虹彩（アイリス）の模様をいう。虹彩は、脈絡膜が伸びて出来たもので、放射状に瞳孔開大筋、輪状に瞳孔活躍筋が並ぶ。光に対して反射的に働き、瞳孔の開閉や明暗調節を行う。含まれる色素によって茶眼、青眼等になる。

尚、認証は、上述した人間の生物学的特徴にとらわれず、顔写真、署名等の筆跡を用いても構わない。

【００２２】

説明を図１に戻す。５はエンドユーザであり、エンドユーザ５が持つ携帯通信端末装置５１、例えば、携帯電話、ＰＤＡ（Personal Data Assistants）等のモバイル機器は、銀行営業システム１が持つＡＴＭ機器１１、ならびに流通系システム２が持つホスト２１とは、公衆回線網６経由で接続される。また、公衆回線網６に接続されないシステムとして自動販売機システム７があり、携帯通信端末装置５１とは、後述するようにオフラインで接続される。

尚、上述した銀行、流通系のシステム１、２は、電子通貨発行、運用のための電子通貨発行運用組織に加盟してあるものとし、エンドユーザ５としての個人は、後述するように、携帯通信端末装置５１を使用して自身で持つ口座預金の中か

ら必要金額だけ電子通貨に交換して引き落とし、その貨幣的価値情報をあらかじめ内蔵する記憶装置に設定してあるものとする。

ここで、電子通貨は、円やドルなどの基軸通貨に連動させてあるものとする。電子商取引には、商品の取引に加えて役務の取引も含まれる。商品には、銀行や証券会社が取り扱う金融商品も含まれる。

【００２３】

図２は、図１における携帯通信端末装置５１の内部構成を示すブロック図であり、ここでは携帯電話端末が例示されている。図２に示すように、携帯電話端末は、基本的には、ＲＦ回路５１１、ＤＳＰ（Digital Signal Processor）を核とするベースバントＬＳＩ５１２、マイクロプロセッサ５１３、入出力インタフェース回路５１４、ＬＣＤパネル５１５、キーボードマウス５１６、フラッシュメモリ５１７、メモリカード５１８、指紋認識力ード５１９で構成される。

【００２４】

ベースバンドＬＳＩ５１２、マイクロプロセッサ５１３、入出力インタフェース回路５１４、フラッシュメモリ５１７は、内部バス５２０を介して共通に接続される。また、入出力インタフェース回路５１４には、更に、ＬＣＤパネル５１５、キーボードマウス５１６、メモリカード５１８、指紋認識カード５１９が接続され、このメモリカード５１８ならびに指紋認識カード５１９は、携帯電話端末本体が持つカードスロットに着脱自在に実装されるものとする。ここでは、カードスロットとしてＰＣカード規格に準拠したものを想定する。

【００２５】

本発明実施形態では、指紋認識カード５１９として、富士通電装株式会社によつて市販されている「Finger Pass Card」を使用するものとする。この指紋認識カード５１９は、ＰＣカードスロットの標準であるＰＣＭＣＩＡタイプIIに準拠するインタフェースを有し、スキャナとの一体化により、１０００～１００００ユーザの指紋データを簡単に登録でき、照合のレベルに合わせて確実に照合が可能である。登録時にカードの末端（ＰＣカードスロット接続部と対向する側）に位置するスキャナ部分に指を押圧し良好な指紋を登録しておけば照合時に良好な結果が得られる。ここでは、指紋の模様に含まれる特徴点の相対的なつながりを

利用して本人か他人かの識別精度を向上させる特徴相関法を用い特徴抽出を行っている。

尚、指紋認識カード５１９を用いることなく携帯通信端末装置５１本体のみで指紋認識を行うことも可能である。この場合、ＬＣＤパネル５１５の少なくとも一部領域は、タブレットと一体型の構成となっており、後述するように、その領域に指を押圧することにより指紋データが採取され、本体内蔵の認識ドライバ（ソフトウェア）がこれを認識（特徴抽出）して外部にある認証サーバ３２へ送信して照合操作を促す。

また、フラッシュメモリ５１７には、後述するプログラムや個人情報、場合によっては既に採取され、登録された指紋パターンが格納されており、メモリカード５１８には、プログラムによって処理されるデータが格納されるものとする。

【００２６】

図３は、本発明実施形態の動作を説明するために引用したフローチャートであり、具体的には、携帯通信端末装置５１が持つフラッシュメモリ、および流通系システム２にプログラムされ記録されるソフトウェアの処理手順を示すものであり、本発明と関係する部分のみ抽出してある。

【００２７】

以下、図３に示すフローチャートを参照しながら、図１、図２に示す本発明実施形態の動作について詳細に説明する。

まず、エンドユーザ５である個人は、自身の携帯通信端末装置５１（つまり携帯個人認証装置）を使ってＡＴＭオンラインシステムを利用し、あるいはインタネットに接続して銀行を含む各企業が提供するサービスシステムをアクセスする（ステップＳ３１）。いずれも公衆回線網６を介してアクセスする。

ここでは、例えば、流通系の百貨店における商品メニューの表示を要求したとする。携帯通信端末装置５１は、その要求に従う商品メニューを検索して流通系システム２から受信（ステップＳ３２）した後、購入したい商品を選択し、その商品名と共に決済の仕方に関しキーボードマウス５１６を介して指示する（ステップＳ３３）。

【００２８】

このことにより、通信機器５１内蔵のマイクロプロセッサ５１３は、フラッシュメモリ５１７にあらかじめ記録されてある個人情報領域をアクセスし、キャッシュ決済の場合は個人の識別番号（口座番号でも可）を、クレジット決済の場合はそのクレジット情報（ユーザ識別番号）をインタネット経由でサービスを提供している流通系企業へ送信する（ステップＳ３６、Ｓ４５）。

【００２９】

ここで、キャッシュ決済の場合、支払金額とメモリカード５１８に設定され、格納されてある価値残高情報との比較（ステップＳ３８）を行う。そして、その残高範囲内にあれば相当金額を引き出し（ステップＳ４２）商談は成立する。ない場合は、引き落とす旨利用者に確認し、ＡＴＭ機器１１を介して銀行に接続して残高照会を行い、銀行預金口座に対する認証（ステップＳ４０）を行い、メモリカード５１８に対して所定金額の補充（ステップＳ４１）を行なう。そして先の引き出しで満たない金額相当を引き落とす（ステップＳ４２）。そして、初期の価値情報、残高、支払い実績等に関する情報を更新し、メモリカード５１８中に履歴として残す。

【００３０】

ここで、銀行預金口座に対する認証は、利用者がパスワードを入力する手間を省くために、携帯通信端末装置５１がフラッシュメモリ５１７の固定領域に書き込まれている個人情報領域をアクセスすることにより取引銀行に自動的に送信するものとする。または、利用者に対し、携帯通信端末装置５１が持つ指紋認識カード５１９のセンサ領域に指を押圧することを促し、この結果、指紋認識カード５１９により、または指紋認識力ード５１９を介して取込まれた指紋情報を受信して照合処理を行う。この照合処理は、銀行計算センタにある認証サーバ３２で行われ、口座開設に際しあらかじめ採取された指紋情報との照合操作がなされ、自動的に認証が行われる。

尚、既に指紋が採取されフラッシュメモリ５１７の特定領域に格納されている場合は上記した手間を省くためにその登録済みの情報を自動的に送信する方法を採用しても良い。

【００３１】

クレジット決済に関しても同様、フラッシュメモリ５１７の固定領域にカード識別番号等の個人情報が書き込まれており、この領域の内容をカード会社へ送信して認証の結果を得る。または、利用者に対し、携帯通信端末装置５１が持つ指紋認識力ード５１９のセンサ領域に指を押圧することを促し、この結果、採取された指紋情報を受信して照合処理を行う。照合処理は、銀行計算センタ３にある認証サーバ３２に委ねるか、あるいは独自に用意するデータベースを用いて行われる。

【００３２】

ここで、あらかじめ採取された指紋情報との照合操作がなされ、自動的に認証が行われる。カード会社は、カード識別番号あるいは指紋が適正か、また、希望商品を購入した場合、取引限度額を超えないか調べ、（ステップＳ４６、Ｓ４７）その商品の受注処理へ進む。

尚、残高照会の結果、支払金額に見合う金額が預金口座にない場合は支払い不能とし、その旨、携帯電話５１が持つＬＣＤパネル５１５に表示（ステップＳ４３）して商談は不成立となる。また、クレジットに関しても残高不足の場合は支払い不能とし、その旨表示して商談は不成立となる。

【００３３】

発注を受けた流通系企業では、その発注情報を受信することによって在庫を調べ、ある場合は決済処理を終了した旨と合わせて要求のあった通信機器５１にインタネット経由で返答し、ない場合は、現在発注された商品在庫がない旨、更に入荷予定日をインタネット経由で携帯通信端末装置５１に返答する。

【００３４】

尚、携帯通信端末装置５１が持つメモリカード５１８は、携帯通信端末装置５１本体が持つＰＣカードスロットに実装され、必要に応じて取り外し、たとえば、自動販売機システム７が持つカードスロットに装填することにより自販機支払いのための処理を行うことができる。また、ＡＴＭ機器１１が持つカードスロットに実装することによっても電子通貨の交換をローカルに実行できる。

【００３５】

図４は、本発明の携帯個人認証装置が携帯通信端末装置として使用される通報

システムの実施形態を示すブロック図である。図４は、自動車事故が発生したときに自動車４１（４２、４ｎ）から自動的にＳＯＳ信号を発し、警察や消防、あるいは保険会社等所轄のセンタ４５に緊急通報するシステムである。ここでは、全地球測位システム（ＧＰＳ：Global Positioning System）の衛星電波を受信できるカーナビゲーションシステムを構成要素とする機器（通報システム搭載機器４１１）を各自動車４１（～４ｎ）に搭載し、緊急時に現在位置を知らせるＳＯＳ信号を携帯電話回線４３経由で発信する仕組みを用いている。

具体的には、交通事故等でエアバッグが作動すると、搭載機器がＧＰＳにより測位された現在位置や車体番号等の情報を自動的に発信する。これを２４Ｈ体制のサービス会社４４がキャッチし、自動車の位置やドライバの氏名、住所、自動車の番号を事故事に最も近い警察局や消防署（所轄センタ４５）に通報する。これは事故のみならず、ドライバが運転中に急病で発作を起こした場合にも手動で発信できるものとし、また、搭載機器は事故の衝撃にも耐えられるような航空機のフライトレコーダなみの強度を持つものとする。なお、ＧＰＳの衛星電波を受信できない場合は、カーナビゲーションシステムが備える光ファイバジャイロからのデータ、走行距離データなどと地図データを用いたマップマッチングにより、現在位置を知る。

【００３６】

上述した構成において、エアバッグ等が作動しても事故が軽微な場合もあり、また、機器の誤作動もある。この場合、運転者本人がこの通報システムを解除すれば問題は生じないが、大事故の場合、誰かが誤って、あるいは故意に解除することがありえる。このときに上述した個人認証機能を持つ携帯通信端末装置５１（携帯個人認証装置）を使用して本人認証が行われ、サービス会社４４を介して、あるいは所轄のセンタ４５経由で解除の資格チェックが行われる。

認証のしくみについては図１に示す電子商取引システムと同様であり、重複を避ける意味でここでは述べないが、指紋は都度採取せず、あらかじめ内蔵するフラッシュメモリ５１７中に登録しておき、通報時、その情報を自動送信するしくみが必要となる場合もある。

【００３７】

尚、上述した実施形態では携帯通信端末装置５１を兼ねる携帯個人認証装置として携帯電話端末を例示して説明したが、携帯電話端末に限らず、図２に示す基本構成を有するＰＤＡ等各種モバイル機器で代用しても構わない。また、本発明実施形態では、本人認証のために指紋を用いたが、他に、声紋、虹彩紋、網膜紋、顔、署名等、生物学的特徴を有し、本人認証のために実績を有するものであれば代替することができる。

【００３８】

更に、指紋を採取、照合する手段として、市販の指紋認識カード５１９を携帯通信端末装置５１が持つカードスロットに実装する例のみ示したが、これに制限されることなく、携帯通信端末装置本体にその機能を内蔵しても構わない。特に、最近のＰＤＡの中には、表示入力一体型のものが多く、この場合、画像認識のための機能を本体に内蔵することが多い。従ってＰＤＡ本体に指紋認識のためのソフトウェアを持つことにより、ＰＤＡそのもので代用しても構わない。

また、電子通貨の記憶媒体としてメモリカード５１８のみ例示したが、これに制限されることなく、通信機器５１本体に着脱自在に実装でき、リードライト可能なものであればその種類を問わない。

【００３９】

尚、本発明実施形態では、携帯個人認証装置を携帯通信端末装置として電子商取引システム、通報システムに適用した場合のみ説明したが、これに制限されず、自動車のリモコンによるキーレスエントリの代用として利用可能である。また、個人の認証だけに携帯個人認証装置を使用しても良い。例えば、警察等により不審尋問された場合の認証等種々利用可能である。また、警察や警備会社などが不信尋問を行う際の不審者の特定に使用しても良い。この場合、リファレンスとなる参照データを、携帯個人認証装置内に備えても良いし、前記実施形態のごとく認証サーバ内に備えても良い。また、通報システムとしての応用も多数考えられ、自動車事故はもとより、海山での遭難事故等にも威力を発する。

また、ＥＴＣにおける車載装置の作動許可や、定期券の券売機などの自動販売機をはじめ、個人認証を前提としたあらゆる電子システムに適用することができる。

【００４０】

【発明の効果】

以上説明のように本発明の携帯個人認証装置によれば、あらゆる用途に使用できる。本人認証のための手段として、指紋、声紋、虹彩紋、網膜紋、顔、署名等の生物学的特徴を用いることによってセキュリテイ機能の充実がはかれる。

また、本発明の携帯個人認証装置にＩＣカード、クレジットカード等が持つ機能を内包させ、例えばＡＴＭ機器と接続することにより、携帯個人認証装置を財布化して一元管理でき、また、各企業が構築するサービスシステムを取込むことによって各種商取引を簡単に実現できる。また、ＩＣカードを電子通貨の媒体とする場合に比較して、パスワード入力等の煩わしさから解放される。更に、通信機器が持つ記憶装置内に使用履歴が都度格納され、必要に応じて残高等表示パネルにビジュアル表示されるため、履歴を含む現状把握が可能となり、利便性に富む。

【００４１】

更に、交通事故、遭難事故等発生の際、所轄センタへの緊急連絡解除時の本人認証のための手段としても本発明の携帯個人認証装置を用いることができる。この場合、全地球測位システム（ＧＰＳ）の衛星電波を受信できる機器などを介して現在位置等を知らせるＳＯＳ信号を任意の通信手段で所轄のセンタに通報するが、緊急連絡解除の際に携帯個人認証装置による通信手段で通信を行い、本人認証を受ける。これにより、機器の誤作動による、あるいは悪意の緊急連絡解除を防止することができ、このことにより、通報の確度が向上する。

【図面の簡単な説明】

【図１】　本発明の一実施形態を示すブロック図である。

【図２】　図１における携帯個人認証装置（携帯通信端末装置）の内部構成を示すブロック図である。

【図３】　図１に示す本発明の一実施形態の概略動作を示すフローチャートである。

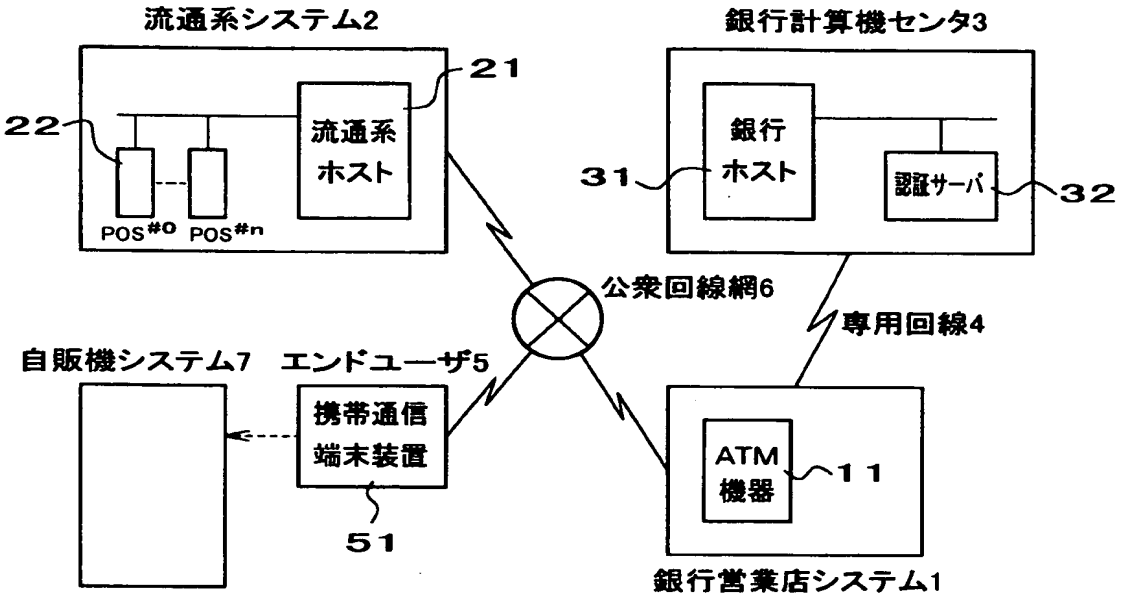
【図４】　本発明の他の実施形態を示すブロック図である。

【符号の説明】

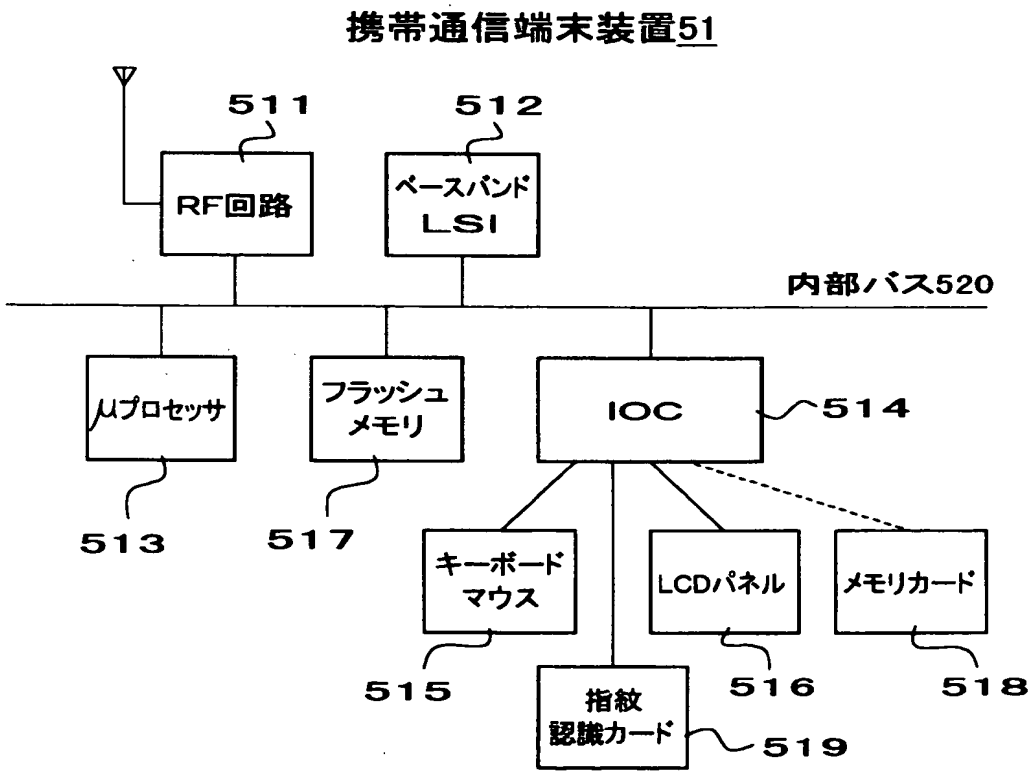
１…銀行営業店システム、２…流通系システム、３…銀行計算機センタ、４…専用回線、５…エンドユーザ、６…公衆回線網、７…自動販売機システム、１１…ＡＴＭ機器、２１…流通系ホスト、３１…銀行ホスト、３２…認証サーバ、４１（４２、４ｎ）…自動車、４３…携帯電話回線網、４４…サービス会社、４５…所轄センタ、５１…携帯通信端末装置（携帯個人認証装置）、５１１…ＲＦ回路、５１２…ベースバンドＬＳＩ、５１３…マイクロプロセッサ、５１４…入出力コントローラ、５１５…ＬＣＤパネル、５１６…キーボードマウス、５１７…フラッシュメモリ、５１８…メモリカード、５１９…指紋認証カード、５２０…内部バス

【書類名】　　図面

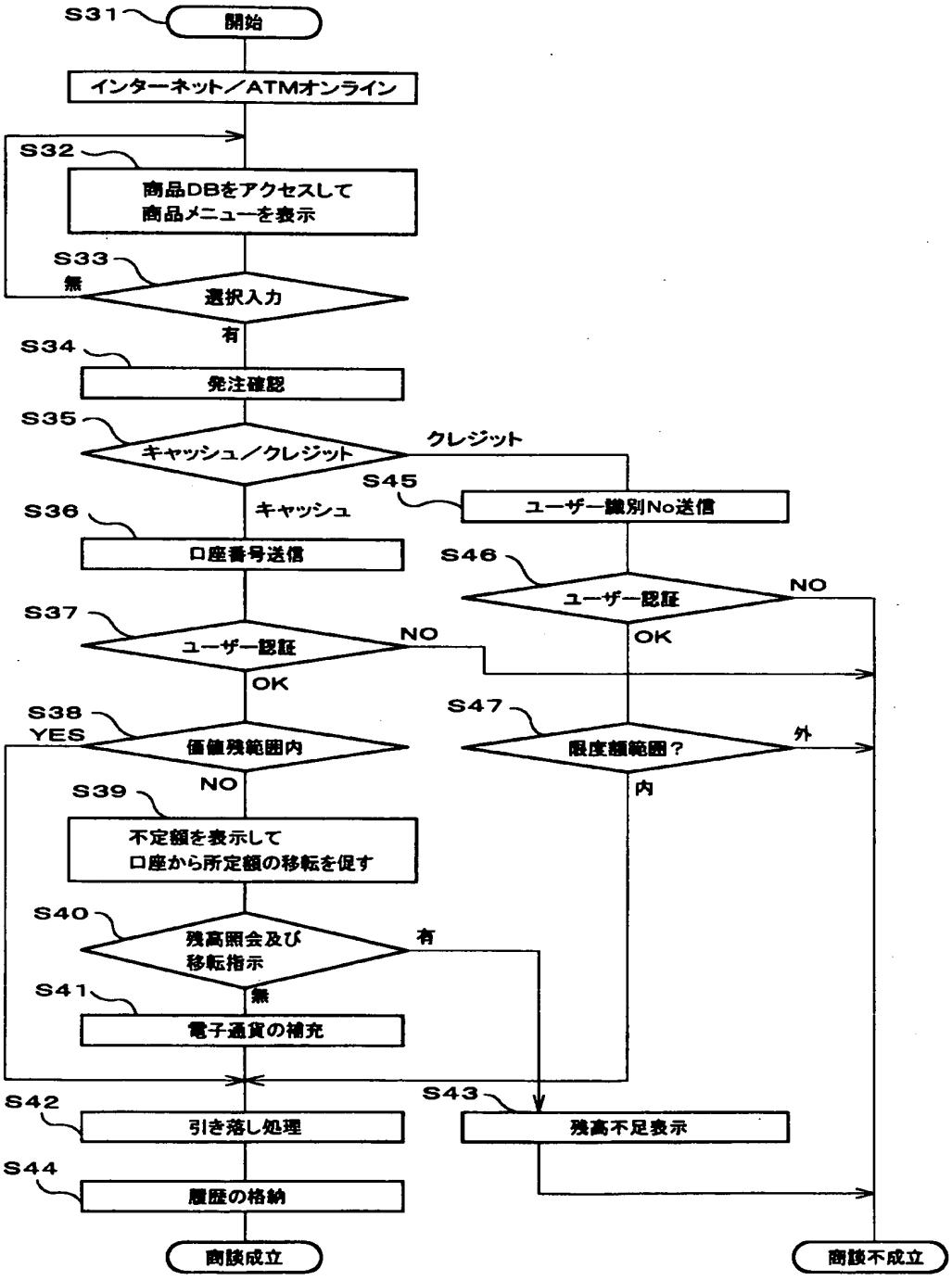
【図１】


流通系システム2
銀行計算機センタ3
21
22
流通系
ホスト
POS#0
POS#n
31
銀行
ホスト
認証サーバ
32
公衆回線網6
専用回線4
自販機システム7
エンドユーザ5
携帯通信
端末装置
51
ATM
機器
11
銀行営業店システム1

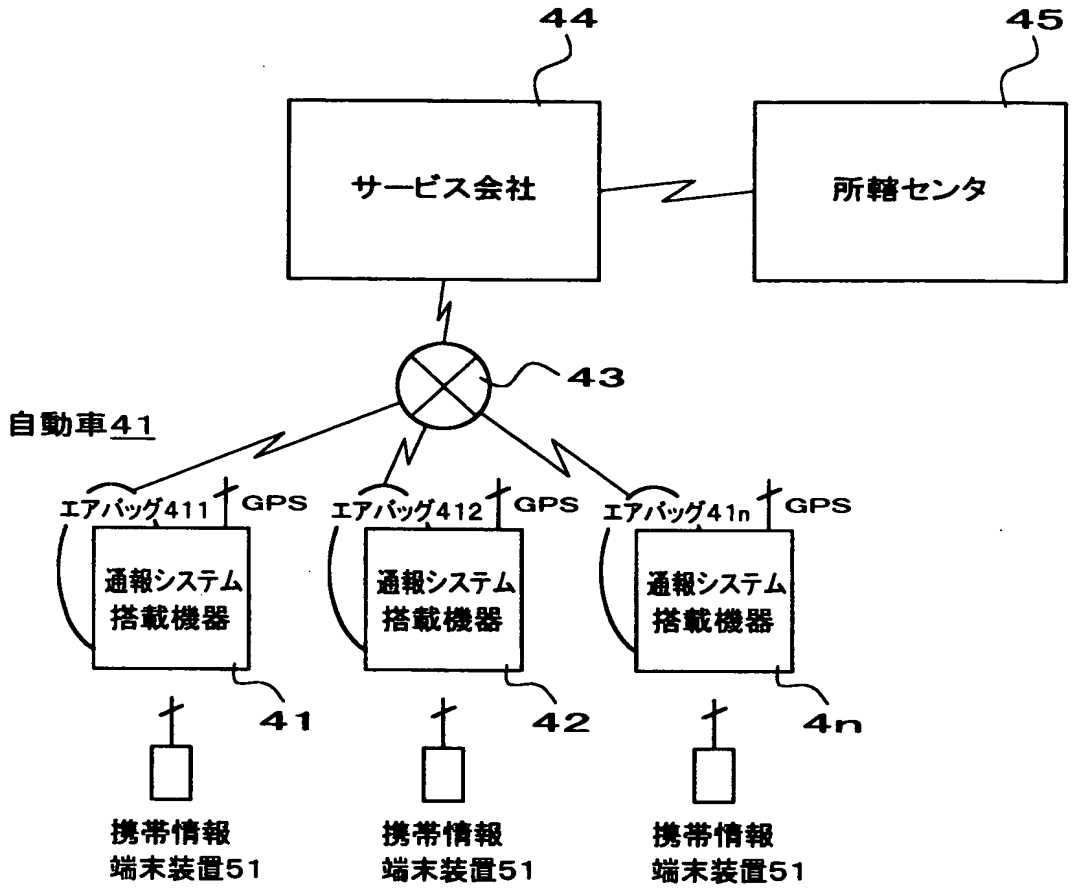
【図２】


携帯通信端末装置51
511
512
RF回路
ベースバンド
LSI
内部バス520
μプロセッサ
フラッシュ
メモリ
IOC
514
513
517
キーボード
マウス
LCDパネル
メモリカード
515
516
518
指紋
認識カード
519

【図３】


S31
開始
インターネット／ATMオンライン
S32
商品DBをアクセスして
商品メニューを表示
S33
無
選択入力
有
S34
発注確認
S35
キャッシュ／クレジット
クレジット
S45
ユーザー識別No送信
キャッシュ
S36
口座番号送信
S46
ユーザー認証
NO
OK
S37
ユーザー認証
NO
OK
S38
YES
価値残範囲内
S47
限度額範囲？
外
内
NO
S39
不定額を表示して
口座から所定額の移転を促す
S40
残高照会及び
移転指示
有
S41
無
電子通貨の補充
S42
引き落し処理
S43
残高不足表示
S44
履歴の格納
商談成立
商談不成立

【図４】


44
45
サービス会社
所轄センタ
43
自動車41
エアバッグ411
GPS
エアバッグ412
GPS
エアバッグ41n
GPS
通報システム搭載機器
通報システム搭載機器
通報システム搭載機器
41
42
4n
携帯情報端末装置51
携帯情報端末装置51
携帯情報端末装置51

【書類名】　　要約書

【要約】

【課題】　今後の社会において必要不可欠となる個人の認証をどこでも行え、あらゆる用途に使用することのできる携帯個人認証装置及び同装置によりアクセスが許可される電子システムを提供することを目的とする。

【解決手段】　携帯個人認証装置を携帯通信端末装置５１として、携帯電話やＰＤＡ等のモバイル機器を使用し、生物学的特徴である、指紋、声紋、虹彩斑等のバイオメタリクス認証のうち少なくとも１つを本人認証のための手段として用いる。また、携帯通信端末装置（携帯個人認証装置）に従来ＩＣカード等が持っていた電子財布的な機能を内包させ、ＡＴＭ機器等と接続することによって電子財布としての一元管理を実現する。更に、携帯通信端末装置（携帯個人認証装置）を通報システムにおける緊急連絡解除のための本人認証に使用して通報の確度向上をはかる。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００１６８２０７〕

１．変更年月日　　１９９７年　６月１１日
　［変更理由］　住所変更
　　住　所　　千葉県市川市菅野１－２１－２
　　氏　名　　溝部　達司

出　願　人　履　歴　情　報

識別番号　　〔５９６１３２９０５〕

１．変更年月日　　１９９６年　９月１０日
［変更理由］　新規登録
住　所　　東京都小金井市中町２－２２－２８－２１１
氏　名　　澤口　高司